REMARKS

The specification has been amended on page 3 to correct the typographical error noted by the Examiner.

Claims 1–14 are currently pending in the application. The indication that claims 2–14 are directed allowable subject matter, subject to being rewritten in independent form, including all of the limitations of the base claim and any intervening claims, and subject to overcoming the rejection of the base claim under 35 U.S.C. §112, second paragraph, is noted with appreciation. In response to the Examiner's objection that claims 2–14 are dependent from rejected claim 1, claims 2 and 5 have been rewritten in independent form. However, as will be discussed below, no amendment is believed necessary to the base claim 1. As a result of these amendments, claims 3 and 4 depend from independent claim 2, and claims 6–14 depend from independent claim 5. In view of these amendments and the remarks which follow, claims 2–14 are now be in condition for immediate allowance.

The claimed invention in general, and claim 1 in particular, enables anonymous electronic communication and double-blind transactions in which sender and recipient correspond with each other through pseudonyms. Neither the sender nor the recipient of a message is aware of the other's identity or address, and their identities and addresses are concealed from the network via which the message is sent and from local and global eavesdroppers. Concealment from the network and from local and global eavesdroppers increases security in part by concealing the existence of message traffic between the two parties. Each message is passed through a sequence of Forwarding Agents, the order of which is randomly determined, with the result that the actual destination address is not revealed until the message passes through the last Forwarding Agent in the sequence. The identity of a recipient is thus not revealed by the compromise of any single Forwarding Agent, because no single agent can establish a correlation between a pseudonym and a

destination address.

Claim 1 was rejected under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential steps. In support of his rejection, the Examiner cites MPEP 2172.01. Specifically, the Examiner takes the position that the omitted steps are decryption steps for uncovering a client's network address from the onion address of the client. This rejection is respectfully traversed for the reason that claim 1, as presented, includes all essential steps.

The Examiner takes the position that the omitted steps are "decryption steps for uncovering a client's network address from the onion address of the client . . ." The Examiner notes that the claim recites "the step of registering an encrypted form of a client's network address, rendering it unreadable to any individual FA . . ." but later in the claim "a Forwarding Agent finds a visible network address . . .". The Examiner also takes the position that the claim appears to be inconsistent in that the "step of uncovering the visible network address by a single FA contradicts the earlier claim [sic] that the encrypted form of the client's network address is unreadable to any individual FA." It is respectfully submitted that the Examiner has confused two different network addresses: the client's network address and the network address where the message is to be delivered.

According to the basic protocol of the system, each client of the system has to initially register with a Forwarding Agent S of his or her choice. The client, having selected a Forwarding Agent S, also picks one of the groups that the Forwarding Agent S belongs to, thus selecting k agents to be associated with the client. This registration process involves the assignment of a pseudonym to the client. The client also provides the Forwarding Agent S with an encrypted form of his or her network address, rendering it unreadable to any individual FA. In other words, it is the client's network address which is unreadable, not the network address to which the message is sent. Each FA maintains a table with three fields, i.e., a pseudonym, a corresponding encrypted network address and

the FA group to be used for forwarding. The system delivers a message as follows. A message meant for a pseudonym X arrives at the FA where X is registered. The message then goes through a random sequence of FAs. The set of FAs through which the message passes is fixed for each pseudonym. The last FA in the sequence finds a visible network address and sends the message on to this address.

Applicant respectfully submits that the Examiner has misapprehended the claim, because the claim makes it clear both (a) that the visible network address to which the message is sent is uncovered by passing the message through a random sequence of Forwarding Agents and (b) that this network address is not revealed until the message has passed through the last Forwarding Agent in the sequence, rather than passing through a single Forwarding Agent:

> "passing the message through a random sequence of FAs in the group to which Forwarding Agent S belongs; and
>
> finding by the last FA in the sequence a visible network address and sending the message on to this address."

Claim 1, *supra*, lines 23-26. In this regard, the claim closely tracks the specification, which provides, for example:

> A message meant for a pseudonym X arrives at the FA where X is registered. The message then goes through a random sequence of FAs. The set of FAs through which the message passes is fixed for each pseudonym. The last FA in the sequence finds a visible network address and sends the message on to this address.

Specification, page 6, Lines 14–18. Thus, it is apparent that claim 1 neither omits essential matter nor contains internally inconsistent steps.

In view of the foregoing, it is respectfully requested that the rejection under 35 U.S.C. §112, second paragraph, be reconsidered and withdrawn.

Claim 1 was also rejected under 35 U.S.C. § 103(a) as unpatentable over M.G. Reed, P.F. Syverson, and D.M. Goldschlag, "Anonymous Connections and Onion

Routing", *16 IEEE Journal on Selected Areas in Communications* 482 (May 1998) (hereinafter, "Reed, Syverson, and Goldschlag"), in view of M. K. Reiter and D. Rubin, "Crowds: Anonmity for Web Transactions", 1 *ACM Transactions on Information and System Security* 66 (November 1998) (hereinafter, "Reiter and Rubin"), and in futher view of B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (2d ed. 1996) (hereinafter "Schneier"). This rejection is respectfully traversed on the basis that claim 1 is not obvious and is patentably distinct from the prior art, and on the basis that the Examiner's view of prior art reflects the benefit of impermissible hindsight vision afforded by the claimed invention.

Applicant respectfully submits that the Examiner has failed (a) to consider the claimed invention as a whole, (b) to consider the references as a whole to determine whether such references suggest the desirability and thus the obviousness of making the combination, (c) to view the references without the benefit of impermissible hindsight vision afforded by the claimed invention, and (d) to determine obviousness according to the standard of reasonable expectation of success. *See* MEP § 2141.

The concealment of destination addresses from the sender was not a feature of the prior art and would not have been obvious, absent impermissible hindsight, to a person having ordinary skill in the art. Taking the references as a whole, there does not appear to be anything to suggest the desirability of combining them to arrive at the claimed invention; nor is there anything to suggest that one having ordinary skill in the art would arrive at the claimed invention by combining the references cited by the Examine. The claimed invention is not obvious under 35 U.S.C. § 103(a).

Reed, Syverson, and Goldschlag are concerned with internet applications in which the sender typically knows the web page being accessed or the email address to which a message is being sent. Reed, Syverson, and Goldschlag thus describe techniques for concealing the identity of a sender from a recipient and the identity of a recipient from a network via which a message to such recipient is sent, but Reed, Syverson, and

14

Goldschlag do not provide a way of concealing the recipient's identity or address from the sender. Reed, Syverson, and Goldschlag, in fact, require the sender to know the recipient's identity and address in order to access a web page of send a message. As a result, the techniques described by Reed, Syverson, and Goldschlag are not suitable for communication with sender anonymity or double-blind transactions, which are objects of the claimed invention. The Examiner notes that "Reed is silent on the matter of each Forwarding Agent belonging to at least one group, wherein the client selects one of these groups and a message is passed randomly to a subset of FAs of the group," but the Examiner fails to point out that the very feature observed to be missing from Reed, Syverson, and Goldschlag is a principal feature making the claimed invention possible. It is principally by passing a message through a random sequence of FAs, such that passage through the last FA in the sequence reveals a visible network address and sends the message to that address, that the claimed invention makes it possible to conceal the identity of a recipient from a sender and from a network via which a message is sent. The Examiner thus acknowledges that Reed, Syverson, and Goldschlag are silent on at least one principal feature distinguishing the claimed invention from prior art.

The Examiner relies on Reiter and Rubin to make up for the deficiencies of Reed, Syverson, and Goldschlag, notwithstanding the fact that the Crowds system of Reiter and Rubin provides sender anonymity but not recipient anonymity. As discussed in the specification, the Crowds system consists of a cooperative group of users providing sender anonymity, as well as recipient anonymity against local eavesdroppers and colluding forwarders known as "jondos." The Crowds system is primarily designed for anonymous access to web pages where it is understood that the sender knows the location of the page to be accessed. As a result, the Crowds system does not envisage providing the recipient with anonymity against the sender. Unlike the Crowds system of Reiter and Rubin, the claimed invention provides recipient anonymity against the sender by requiring the sender to address the message to a pseudonym. A combination of Reed,

Syverson, and Goldschlag with Reiter and Rubin would not result in the claimed invention.

Recognizing that neither Reed, Syverson, and Goldschlag nor Reiter and Rubin anticipate the claimed invention, the Examiner relies on the Schneier treatise. However, Schneier discusses applied cryptography in terms of concealing message contents and not in terms of concealing message senders or recipients. Cryptographic techniques such as public key encryption or the use of multiple keys, which are discussed by Schneier, are discussed without reference to or consideration of problems relating to concealing the identity or address of a sender or a recipient of a message, either from each other or from a network via which a message is sent (or eavesdroppers on such a network). Schneier does not, therefore, anticipate the claimed invention, either standing alone or in combination with Reed, Syverson, and Goldschlag or Reiter and Rubin.

It is not reasonable to assume that a person of ordinary skill in the art, who was handed Reed, Syverson, and Goldschlag, plus Reiter and Rubin, plus Schneier, would (a) identify an unsolved problem for which they could be combined to create a solution or (b) be able to solve the problem of concealing the identity or address of a sender or a recipient of a message, either from each other or from a network via which a message is sent (or eavesdroppers on such a network) by arriving at the claimed invention. The Examiner's view that the claimed invention is obvious in view of Reed, Syverson, and Goldschlag, in view of Reiter and Rubin, and in further view of Schneier thus appears to be based less on objective consideration of the references taken as a whole and more on impermissible hindsight afforded by the claimed invention. Claim 1 should be allowed.

In view of the foregoing, it is respectfully requested that the application be reconsidered, that claim 1 be allowed together with claims 2–14, and that the application be passed to issue.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone

number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

Applicant hereby makes a written conditional petition for extension of time, if required. Please charge any deficiencies in fees and credit any overpayment of fees to Attorney's Deposit Account No. 50-2041 (Whitham, Curtis & Christofferson).

Respectfully submitted,
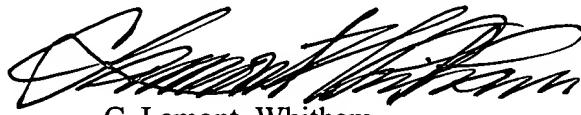
C. Lamont. Whitham
Registration No. 22,424

Whitham, Curtis & Christofferson, P.C.
11491 Sunset Hills Road, Suite 340
Reston, Virginia 20190
Tel. (703) 787-9400
Fax. (703) 787-7557
Customer No.: 30743